UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,070	02/01/2002	Satyendra Yadav	10559-754001	2485

20985 7590 09/05/2007
FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
09/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/066,070	YADAV, SATYENDRA	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20 and 29-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *21-28* is/are allowed.

6)☒ Claim(s) *1-20,29 and 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/5/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/5/2007 has been entered.

Response to Arguments

3. Applicant's arguments filed 6/5/2007 have been fully considered but they are not persuasive.

The arguments of 6/5/2007 did not explain much regarding the specifics why Trostle and Gluck fail to read on the claimed invention. Thus, examiner points to applicant's argument of 11/17/2006 on page 11. Applicant argues Trostle's invention of

detecting the application is during pre-boot, which teaches away from the claimed invention of examining already invoked applications. However, applicant admits that Trostle's background clearly teaches the detection program after invoking the application, which even though is Trostle's background (col.1, lines 39-57) of the invention is still considered as prior art. Therefore, argument with respect to claims 1-20 and 29-30 are not persuasive. Claims 1-20 and 29-30 remains rejected over the Trostle and Gluck combination.

4. Applicant's arguments filed 6/5/2007, with respect to claim 21 have been fully considered and are persuasive. The rejection of claims 21-28 has been withdrawn. Thus, they are in condition for allowance.

Allowable Subject Matter

5. Claims 21-28 are allowed over art.

Claims 21-28 has overcome the prior art including Trostle and Gluck. Claim 21-28 recites the allowable feature of examining a set of instructions embodying an invoked application to identify the invoked application, obtaining application-specific intrusion criteria, and monitoring network and the obtaining using the application-specific intrusion criteria to detect an intrusion.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-20, 23 and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle (US 5,919,257) and in further view of Gluck, et al. (US 5,948,104).

As per claim 1:

Trostle discloses a machine-implemented method comprising:

examining a set of instructions embodying an invoked application **[COL.2, lines 33-34]** to identify the invoked application; **[COL.5, lines 21-23; Trostle discloses the pre-boot modules as the claimed invoked application.]**

monitoring network communications for the invoked application, after the examining and the obtaining **[COL.1, lines 39-54]**, *[using the application-specific intrusion detection signature]* to detect an intrusion. **[COL.2, lines 49-67 and COL.6, lines 54-62; The claimed application-specific criteria to detect intrusion is broad and can broadly be given to any information that is specific to the application where this information verifies whether the application is authentic or not. If not, the application has been replaced or modified which is a sign of intrusion. Thus,**

application-specific intrusion criteria can broadly be given in light as a hash that is specific to the application because the hash value has to match to the trusted hash value (COL.2, lines 49-67 and COL.6, lines 54-62) or a signature to verify the module is authentic and prevents unauthorized replacement or modifications (col.5, lines 32-36).]

The pre-boot modules (invoked application) of Trostle are signed which is a signature for that specific module to verify if authentic or whether there is an unauthorized replacement or modification to show an intrusion for the module **[col.5, lines 21-23 and 27-36]**. However, Trostle did not include intrusion detection signature.

Gluck is brought forth to teach the limitation intrusion detection signature because Trostle discloses the application specific intrusion criteria. The intrusion detection signature can also be interpreted as a virus signature that contains a signature for that specific type of intrusion (virus). Gluck discloses virus signatures to detect the known characteristic behaviors of viruses **[col.5, lines 45-48]**. Gluck, et al. teaches anti-virus program that detects and remove known viruses where the anti-virus program searches for signatures including characteristic behaviors of viruses and removes any found virus **[COL.1, lines 53-58]**. Gluck teaches the claimed invoked application in the form of installing a program or executed program that contains updated virus signatures files where the scanner will scan or examine the virus signature which are instructions **[COL.3, lines 53-58]**. Gluck teaches the computer system scans all relevant media for known viruses by searching for patterns or

signatures **[COL.5, lines 14-18]** where signatures are sequential portion of code (up to 16 bytes in length) unique to each virus **COL.5, lines 45-50].**

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine intrusion detection of the executed programs of Trostle with an virus signature because a signature of a virus is a sequential portion of code unique to each virus to detect variation of strings of bytes so that helps determine the type of intrusion in order to eliminate the viruses **[Gluck on COL.3, lines 50-54 and COL.5, lines 28-50]**.

As per claim 2: **See Trostle on col.3, lines 19-30;** discussing tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

As per claim 3: **See Trostle on col.5, lines 50-52;** discussing tracking one or more characteristics of the network communications comprises comparing the one or more characteristics with one or more configurable thresholds.

As per claim 4: **See Trostle on col.1 line 66 – col., line 3;** discussing at least one of the one or more configurable thresholds comprises a threshold set by monitoring communications for the invoked application during a defined time window.

As per claim 5: **See Trostle on col.1, lines 39-41;** discussing monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

As per claim 6: **See Trostle on col.4, lines 32-35;** discussing the network intrusion detection system component and the invoked application run within a single execution

context.

As per claim 7: **See Trostle on col.3, lines 8-30 and col.6, lines 13-17;** discussing providing a first application-specific remedy for a detected intrusion; and providing a second application-specific remedy for identified application-specific abnormal communication behavior.

As per claim 8: **See Trostle on col.2, line 66 – col.3, line 2 and col.6, lines 37-38;** discussing providing a first application-specific remedy comprises cutting at least a portion of the network communications for the invoked application, and wherein providing a second application-specific remedy comprises notifying a system administrator of the identified application-specific abnormal communication behavior.

As per claim 9: **See Trostle on col.5, lines 44-45;** discussing obtaining the application-specific intrusion detection signature comprises loading the application-specific intrusion detection signature from a local signature repository.

As per claim 10: **See Trostle on col.5, lines 44-45 and col.6, lines 13-20;** discussing obtaining the application-specific intrusion detection signature comprises: requesting the application-specific intrusion detection signature from a local signature repository in communication with a remote signature repository; and receiving the application-specific intrusion detection signature from the local signature repository.

As per claim 11: **See Trostle on col.2, lines 44-60;** discussing the set of instructions reside in a file, and wherein examining the set of instructions comprises: applying a hash function to data in the file to generate a condensed representation of

the data; and comparing the condensed representation with existing condensed representations for known applications.

As per claim 12:

Trostle teaches a machine-readable medium embodying machine instructions for causing one or more machines to perform operations comprising:

examining a set of instructions embodying an invoked application **[COL.2, lines 33-34]** to identify the invoked application; **[COL.5, lines 21-23; Trostle discloses the pre-boot modules as the claimed invoked application.]**

monitoring network communications for the invoked application, after the examining and the obtaining **[COL.1, lines 39-54]**, *[using the application-specific intrusion detection signature]* to detect an intrusion **[COL.2, lines 49-67 and COL.6, lines 54-62; The claimed application-specific criteria to detect intrusion is broad and can broadly be given to any information that is specific to the application where this information verifies whether the application is authentic or not. If not, the application has been replaced or modified which is a sign of intrusion. Thus, application-specific intrusion criteria can broadly be given in light as a hash that is specific to the application because the hash value has to match to the trusted hash value (COL.2, lines 49-67 and COL.6, lines 54-62) or a signature to verify the module is authentic and prevents unauthorized replacement or modifications (col.5, lines 32-36).]**

The pre-boot modules (invoked application) of Trostle are signed which is a signature for that specific module to verify if authentic or whether there is an

unauthorized replacement or modification to show an intrusion for the module **[col.5, lines 21-23 and 27-36]**. However, Trostle did not include intrusion detection signature.

Gluck is brought forth to teach the limitation intrusion detection signature because Trostle discloses the application specific intrusion criteria. The intrusion detection signature can also be interpreted as a virus signature that contains a signature for that specific type of intrusion (virus). Gluck discloses virus signatures to detect the known characteristic behaviors of viruses **[col.5, lines 45-48]**. Gluck, et al. teaches anti-virus program that detects and remove known viruses where the anti-virus program searches for signatures including characteristic behaviors of viruses and removes any found virus **[COL.1, lines 53-58]**. Gluck teaches the claimed invoked application in the form of installing a program or executed program that contains updated virus signatures files where the scanner will scan or examine the virus signature which are instructions **[COL.3, lines 53-58]**. Gluck teaches the computer system scans all relevant media for known viruses by searching for patterns or signatures **[COL.5, lines 14-18]** where signatures are sequential portion of code (up to 16 bytes in length) unique to each virus **COL.5, lines 45-50].**

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine intrusion detection of the executed programs of Trostle with an virus signature because a signature of a virus is a sequential portion of code unique to each virus to detect variation of strings of bytes so that helps determine the type of intrusion in order to eliminate the viruses **[Gluck on COL.3, lines 50-54 and COL.5, lines 28-50]**.

As per claim 13: **See Trostle on col.3, lines 19-30;** discussing the operations further comprise tracking one or more characteristics of the network communications to identify application-specific abnormal communication behavior.

As per claim 14: **See Trostle on col.1, lines 39-41;** discussing monitoring network communications comprises monitoring network communications in a network intrusion detection system component invoked with the invoked application.

As per claim 15: **See Trostle on col.4, lines 32-35;** discussing the network intrusion detection system component and the invoked application run within a single execution context.

As per claim 16: **See Trostle on col.3, lines 8-30 and col.6, lines 13-17;** discussing the operations further comprise: providing a first application-specific remedy for a detected intrusion; and providing a second application-specific remedy for identified abnormal communication behavior.

As per claim 17: **See Trostle on col.6, lines 37-38;** discussing the first and second application-specific remedies each comprise cutting at least a portion of the network communications for the invoked application.

As per claim 18: **See Trostle on col.5, lines 44-45 and col.6, lines 13-20;** discusses obtaining the application-specific intrusion detection signature comprises: requesting the application-specific intrusion detection signature from a signature repository; and receiving the application-specific intrusion detection signature from the signature repository.

As per claim 19: **See Trostle on col.5, lines 44-45 and col.6, lines 13-20;**

discussing the signature repository comprises a local signature repository in communication with a remote signature repository.

As per claim 20: **See Trostle on col.2, lines 44-60;** discussing examining the set of instructions comprises: applying a hash function to the set of instructions to generate a condensed representation; and comparing the condensed representation with existing condensed representations for known applications.

As per claim 23: **See Gluck on col.5, lines 45-48**; discussing intrusion signature.

As per claim 29:

Trostle teaches a system comprising:

a security operation center; **[COL.2, line 5 – COL.3, line 1 and COL.5, lines 47-48]**

one or more machines **[COL.3, lines 55-59]**, each machine including means for identifying a process, after the examining and the obtaining **[COL.1, lines 39-54]**, and monitoring network communications for the process using the process-specific to detect an intrusion; and **[COL.2, lines 49-67 and COL.6, lines 54-62; The claimed application-specific criteria to detect intrusion is broad and can broadly be given to any information that is specific to the application where this information verifies whether the application is authentic or not. If not, the application has been replaced or modified which is a sign of intrusion. Thus, application-specific intrusion criteria can broadly be given in light as a hash that is specific to the application because the hash value has to match to the trusted hash value (COL.2, lines 49-67 and COL.6, lines 54-62) or a signature to verify the module is**

authentic and prevents unauthorized replacement or modifications (col.5, lines 32-36).]

communication means coupling the one or more machines with the security operation center. **[COL.5, line 66 – COL.6, line 2 and lines 7-13]**

The pre-boot modules (invoked application) of Trostle are signed which is a signature for that specific module to verify if authentic or whether there is an unauthorized replacement or modification to show an intrusion for the module **[col.5, lines 21-23 and 27-36]**. However, Trostle did not include intrusion detection signature.

Gluck is brought forth to teach the limitation intrusion detection signature because Trostle discloses the application specific intrusion criteria. The intrusion detection signature can also be interpreted as a virus signature that contains a signature for that specific type of intrusion (virus). Gluck discloses virus signatures to detect the known characteristic behaviors of viruses **[col.5, lines 45-48]**. Gluck, et al. teaches anti-virus program that detects and remove known viruses where the anti-virus program searches for signatures including characteristic behaviors of viruses and removes any found virus **[COL.1, lines 53-58]**. Gluck teaches the claimed invoked application in the form of installing a program or executed program that contains updated virus signatures files where the scanner will scan or examine the virus signature which are instructions **[COL.3, lines 53-58]**. Gluck teaches the computer system scans all relevant media for known viruses by searching for patterns or signatures **[COL.5, lines 14-18]** where signatures are sequential portion of code (up to 16 bytes in length) unique to each virus **COL.5, lines 45-50].**

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine intrusion detection of the executed programs of Trostle with an virus signature because a signature of a virus is a sequential portion of code unique to each virus to detect variation of strings of bytes so that helps determine the type of intrusion in order to eliminate the viruses **[Gluck on COL.3, lines 50-54 and COL.5, lines 28-50]**.

As per claim 30: See Trostle on col.3, lines 19-30; discussing each machine further includes means for tracking one or more characteristics of the network communications to identify process-specific abnormal communication behavior.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100